

(19) World Intellectual Property Organization
International Bureau



PCT



(43) International Publication Date
23 February 2006 (23.02.2006)

(10) International Publication Number
WO 2006/018427 A1

(51) International Patent Classification: ⁷ **H04L 9/12**

(21) International Application Number:
PCT/EP2005/054004

(22) International Filing Date: 15 August 2005 (15.08.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10 2004 039 899.2 17 August 2004 (17.08.2004) DE

(71) Applicants and

(72) Inventors: **SCHEJA, Katharina** [DE/DE]; Eifelstrasse 3, 65812 Bad Soden (DE). **KOROBKOV, Dmitri** [DE/DE]; Leerbachstrasse 50, 60322 Frankfurt (DE).

(74) Agent: **2K PATENTANWÄLTE KEWITZ & KOLLEGEN PARTNERSCHAFT**; Corneliusstr. 18, 60325 Frankfurt a. M. (DE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

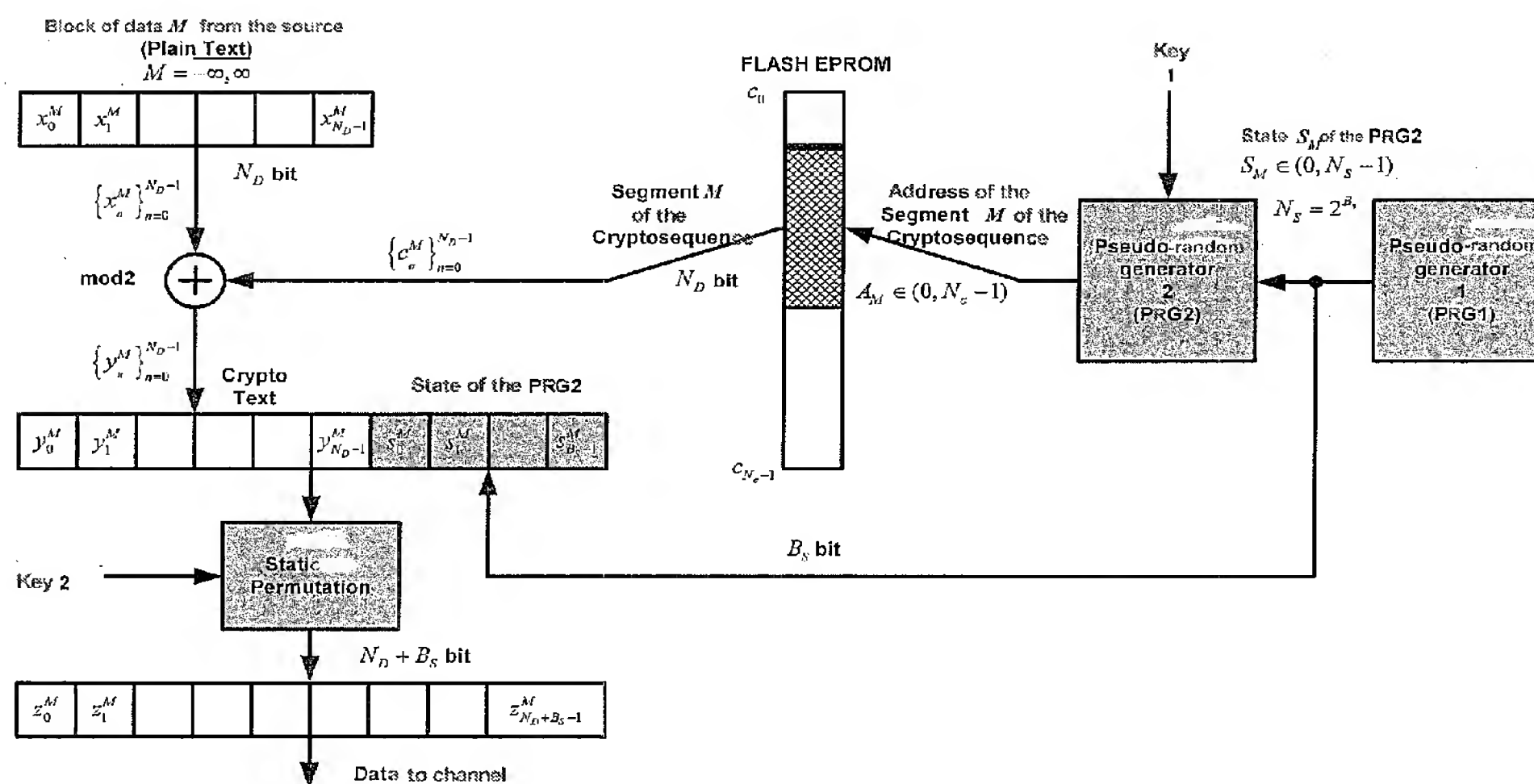
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ENCRYPTION METHOD



(57) Abstract: The present invention relates to a method for encrypting digital information using communication devices, which have an interface for a replaceable or writable storage medium, whose content may be read out and duplicated, having a storage medium which is connected to the interface, a supply of symbols for encryption being stored on the digital storage medium, which may be read out on the basis of an address, having an encryption unit which employs the supply of symbols for encrypting and/or decrypting the digital data stream of the communication device on the basis of at least one address.